UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/274,294	03/22/1999	DAVID GUNTER	MS1-298US	8214

22801 7590 07/29/2002

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
ARANI, TAGHI T	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 07/29/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/274,294	GUNTER ET AL.	
	Examiner	Art Unit	
	Taghi T. Arani	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-20 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-20 were pending for examination.

2. Claims 1-20 are rejected.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 7 recites the limitation "the internal and external clients" in pg. 12, line 12. There is insufficient antecedent basis for this limitation in the claim. For purpose of applying art, the examiner assumes that "an internal" client exchanges encrypted data with an external client over a network and through a firewall intermediate of the internal and external clients.

Claims 8-11 are also rejected by virtue of their dependencies.

4. Claim 3 recites the limitation "signing the encrypted session key using a private key associated with the intermediary" in line 21-22. This limitation compromises the security requirement of the private key and there is insufficient antecedent basis for this limitation in the specification. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). A review of the specification, see pg. 14, lines 1-5, indicates the encrypted session key is signed using one endpoint private key. For the purpose of applying art, the examiner assumes that the encrypted session key is signed using one end-point private key.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefore, subject to the conditions and requirements of this title.

6. Claims 12-15 and 16-18 are rejected under 35 U.S.C. 101 as being directed to non statutory subject matters.

Claim 12 is directed to a network system, an internal client, an external client and an intermediary. A client may be hardware or software. The examiner takes note that claim 12 is directed to a network system but respectfully also notes that the "system" comprises clients which as addressed above could be just software alone, and an intermediary in the preferred embodiment is a firewall which can also be just software alone, hence system could be just software alone.

The examiner asserts that software claims do not fall within any of statutory clauses enumerated in 45 U.S.C. 101.

Claims 13-15 do not add statutory subject matters, but further limits functions performing by the clients or firewall.

Claim 16 is directed to a "software architecture". As recited in the body of the claim, the architechrure comprises various types of code (i.e. software). The examiner respectfully asserts that code does not fall within clauses recited in U.S.C. 101.

Claims 17-18 recite further code functions but add no structure.

Claim Rejections - 35 USC § 102

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

7. The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) do not apply to the examination of this application as the application being examined was not (1) filed on or after November 29, 2000, or (2) voluntarily published under 35 U.S.C. 122(b). Therefore, this application is examined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

8. Claims 1and 4 are rejected under 35 U.S.C. 102(e) as being anticipated by Shwed et al., US Pat. 5,835,726, issued November 1998.

9. Shwed is directed to a system for controlling the flow of data packets in computer networks where a security system for inspecting and selectively modifying inbound and outbound data packets is provided, see col. 3 lines 42-63.

As per claim 1, in an embodiment, Shwed discloses that both endpoints (host 1 and host 2) are connected to their respective private networks. Both endpoints are secured via two firewalls (i.e. intermediaries) though their respective networks (i.e. LANs) and are coupled to a public networks, see col. 14, lines 19-39.

Shwed teaches a packet filter module installed in firewalls where modification, inspection of packets is performed by encryption of outbound packets and decryption of inbound packets, see col. 13, lines 6-20. Shwed uses a Deffie-Hellman key generation for a common secret key B which is used to encrypt the session key R. The same session key R is used for both source and destination to encrypt the data from host1 to host2 and from host 2 to host 1, see col. 16, lines 27-31, see also col. 15, lines 34-67 through col. 16, lines 1-4. That is the session key is securely transferred from one of the end points (i.e.

either host 1 or host 2) to an intermediary (i.e. firewall 2 or firewall1) by encrypting the session key using secret common key B.

Shwed further teaches that an endpoint (i.e. host 1) in sending a packet M to a receiving endpoint (i.e. a host 2), first it generates a signature on the packet and then encrypts it using a function of session key R (i.e. E=R+I) and finally transmits the encrypted packet (i.e. encrypted data stream) over the public network to the receiver endpoint through a firewall (i.e. an intermediary), see col. 18, lines 9-46.

Shewd further teaches that the firewall in receiving endpoint receives the encrypted packet and verifies (or inspects) the encrypted packet through decryption of the encrypted packet and verification of the signature, see col. 18, lines 47-67 through col. 19, lines 1-3.

10. As per claim 4, Shwed teaches this, see col. 3, lines 64-67 through col. 4, lines 1-21. In a preferred embodiment, Schwed's method of operating the security system includes a packet filter module implemented as firewall (i.e. an intermediary) which utilizes the stored data from previous inspections to accept or to reject the passage of the data packets into or out of the computer network. That is, the shwed's firewall must have stored the previous data stream in order to be able to perform the comparison for accepting or rejecting the data packet (or. Stream of data).

Claim Rejections - 35 USC § 103

11. Claims 2, 3 and 5-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shwed et al. as applied to claim 1 above, and further in view of Bruce Schneier, Applied Cryptography, Second Edition, 1996, published by John Wiley & Sons, Inc.

12. As per claim 2, Schwed 's uses 'static" Deffi-Hellman scheme to transfer the session key from the source to the intermediary (i.e. a firewall). The session key R is encrypted using a basic secret common key B which is a function of destination public key, see col. 15, lines 44-67.

However, Schneier teaches a hybrid cryptosystem where public-key cryptography is used to secure and to distribute session key, see pg. 48, lines 8-18.That is, Bob sends Alice his public key. Alice generates a random session key, K, encrypts it using Bob's public key, and sends it to Bob. Bob decrypts Alice's message using his private key. Both of them encrypt their communications using the same session key.

It would have been obvious to one ordinary skill in the art to modify Schwed 's system for controlling the flow of data packets in computer networks to employ Schneier's public key cryptosystem to securely transport the session key (R) from the source (i.e. one end-point) to the intermediary (i.e. the firewall) using intermediary's public key (i.e. the firewall's public key) to take advantage of hybrid cryptosystem in which session key is created when it is needed to encrypt communications and destroyed when it is not longer needed and reducing the risk of compromising the session key, see Schneier, pg. 33, lines 35-40.

13. Claim 3 additionally recite signing the encrypted session key using a private key associated with one endpoint.

Schneier teaches use of digital signature (i.e. signing a message/data stream or document) with public key cryptography. That is, Alice encrypts the message with her private key and sends the signed message to Bob. Bob decrypts the message with Alice's

public key, thereby verifying (or authenticating) the signature, see Schneier, pg. 37, lines 16-30.

It would have been obvious that the source (i.e. host 1) of Schwed signs the session key with its private key to authenticate itself to the firewall (i.e. intermediary), which provides the security of encryption with the authenticity of digital signatures, see Schneier, pg.41,lines 18-30, using sender's private key.

14. Claim 5 in addition to limitations of claims 1-4 recite that public keys of the endpoints and the intermediary are stored at the key storage and decrypting at the intermediary , the signed encrypted session key using one endpoint's public key to return the encrypted session key and decrypting, at the intermediary, the encrypted session key using the intermediary's private key to return the session key.

The examiner notes the reading of Shwed which suggests that firewall maintains a table of bindings between keys and firewalled network objects (i.e. firewalls and clients). That is, a database (i.e. a key storage) within firewall must be configured so that it knows of other potential firewalls and the hosts' (i.e. endpoints) encrypting firewalls. That is, in order to encrypt communications between firewalls, a firewall must have knowledge of its own basic private key and the basic public keys of each firewalled network object it needs to communicate with, see col. 16, lines 5-26.

Furthermore, Schneier teaches a hybrid cryptosystem where public-key cryptography is used to secure and to distribute session key, see pg. 48, lines 8-18.That is, Bob sends Alice his public key. Alice generates a random session key, K, encrypts it

using Bob's public key, and sends it to Bob. Bob decrypts Alice's message using his private key. Both of them encrypt their communications using the same session key.

It would have been obvious to one ordinary skill in the art to modify Schwed 's system for controlling the flow of data packets in computer networks to employ Schneier's public key cryptosystem to securely transport the session key (R) from the source (i.e. one end-point) to the intermediary (i.e. the firewall) using intermediary's public key (i.e. the firewall's public key) to take advantage of hybrid cryptosystem in which session key is created when it is needed to encrypt communications and destroyed when it is not longer needed .

15. Claim 6 additionally recites a computer readable media at one of endpoints and at the intermediary storing computer-executable instructions for performing the method.

Shwed teaches a storage device (i.e. a computer readable media) at the packet filter module (i.e. a firewall or intermediary) for reading and executing the packet filter instructions, see col. 4, lines 10-21.

the examiner asserts that software is the most obvious vehicle to use for performing functions in a computer. Furthermore, it is well known to use computer readable medium to store software. Official notice is taken of motivation to use software (or instructions) would be to allow either the firewall to perform its functions and the end-points to do the same.

16. Claims 7 in addition to limitations of claim 5 recites "authenticating the digital signature as belonging to the internal client ".

The examiner asserts that authenticating the digital signature is well known mechanism used as proof of authorship of the contents of a message. That is, the signature is authentic and convinces the recipient that the signer deliberately signed the message, see Schenier pg. 35, lines 1-10.

It would have been obvious that the firewall would authenticate the digital signature of the internal client to ensure that the data came from the client.

17. Claim 8 recites limitations of claim 7 and 5. It is rejected as such.

18. Claim 9 and 10 in addition to limitations of claim 7 and 1 recites inspecting (claim 9) and storing the data in an unencrypted form (claim 10).

Shwed's packet filter module (i.e. firewall or intermediary) inspects and stores unencrypted, see col. 4, lines 15-21.

19. Claim 11 is an apparatus corresponding to claims 7 and 6. It is rejected as such.

20. Claims 12 differs from claims 1in that the an internal client and an external client configured to communicate encrypted data over a network using virtual private network communication.

Shwed's invention is also providing an encryption scheme for securing the flow of data over insecure public networks, such as the internet forming a virtual private network, see col. 2, lines 62-65

21. Claim13 recites all limitations of claims 12 and 2. It is rejected for the reasons provided in statement of rejection of claims 12 and 2.

22. Claim 14 recites all limitations of claims 12 and 3. It is rejected for the same reasons provided in the statement of rejection claims 12 and 3.

23. claim 15 recites all limitations of claims 12 and 10. It is rejected for the reasons provided in the statement of claims 12 and 10.

24. Claims 16-18 are software architecture corresponding to method claims 1 and 4. Claims 16-18 are rejected as such.

25. Claim 19 is an apparatus corresponding to claim 5. It is rejected as such.

26. Claim 20 is a computer instruction corresponding to claim 1. Claim 20 is rejected.

Conclusion

27. Any inquiry concerning this communication or earlier communications from examiner should be directed to Taghi Arani, whose telephone number is (703) 305-4274. The examiner can normally be reached Monday through Friday from 7:30 AM to 5:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes, can be reached at (703) 305-9711. The Fax numbers for the organization where this application is assigned are:

After-final (703) 746-7238

Official (703) 746-7239

Non-Official/Draft (703) 746-7240

Taghi Arani

Patent Examiner

July 25, 2002

GAIL HAYES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100